PKI AND DIGITAL SIGNATURES

PKI

Public Key Cryptography – Recap

- Key consists of two parts: Pub and Priv
  - Public key for encryption, private key for decryption
  - (Practically) impossible to derive Priv from Pub
- Enc(Data, Pub) -> Ciphertext
- Dec(Ciphertext, Priv) -> Data
- The trick is to use correct public key for encryption
- Reduces big secret to small authentic data

Digital Signature

- Also asymmetric operation with private and public key
- Sign(Data, Priv) -> Signature
- Verify(Signature, Data, Pub) -> Yes/No
- Reduces big authentic data to small authentic data

The Big Question

- **How to distribute public keys in an authentic manner?**

Initial Proposition

- Create a public key file that acts as a telephone book
- File contains all the valid public keys

- Difficult to implement in the 70s

Offline Operation

- Introduce a separate trusted entity: **certification authority**
- Public key of the CA is public knowledge
- CA signs name-key pair
  - Result is called **certificate**
- Certificates can be distributed using untrusted directory
- Certificates can be verified offline
- CA private key is very valuable!

Key Compromise

- Destruction – owner cannot communicate
  - Must get new certificate
- Misuse of key – for limited time, possibility of impersonating key owner and loss of confidentiality
  - Dangerous
- Stealing of key – for unlimited time, impersonating the key owner
  - Very dangerous!

Certificate Revocation

- If private key is compromised, everybody should stop using the corresponding public key
  - Remove the name-key binding
- Directory approach: remove key from directory
- Certificate approach: more complicated because of offline operation

Certificate Revocation List

- CA signs list of revoked certificates
  - Similar to blacklist of invalid credit card numbers
- CRL can also be distributed using untrusted directory
- If party has up-to-date CRL, verification can be done off-line

Problems with CRL

- Can be quite big
  - Estonian ID card CRL: 27MB
  - 757294 revoked and suspended certificates
- Downloading CRLs reintroduces communication problems
- CRLs are not issued at real time – revocation information is delayed

Online Revocation Information

- OCSP – Online Certificate Status Protocol
- Answers queries about revocation status of a single certificate
  - Responses are signed
- Introduces another trusted third party
- Signing responses is computationally costly

Digital Signatures

Required Properties of Signatures

- Is directly connected to signer
- Hard to forge
- Signature on one document cannot be transferred to another document

Requirements to Digital Signatures

- Signature must be represented as digital data
- Signature must depend on signed message
- Signature method must depend on parameter that is unique to the signer and unavailable to other parties
- Signature verification must be able to determine signer without using the mean used for creating signature

The Main Question

- How to create a relation between document and signature that is person-based and easily checked?

The Main Question

- How to create a relation between document and signature that is person-based and easily checked?
- **Unfortunately…** mathematicians have not discovered the existence of „person-based” logical connections between numbers

The Main Question

- How to create a relation between document and signature that is person-based and easily checked?
- **Unfortunately…** mathematicians have not discovered the existence of „person-based" logical connections between numbers
- **Therefore…** connection between person and signature algorithm must be indirect
  - Using an algorithm parameter – **key**

Authentication vs. Digital Signatures

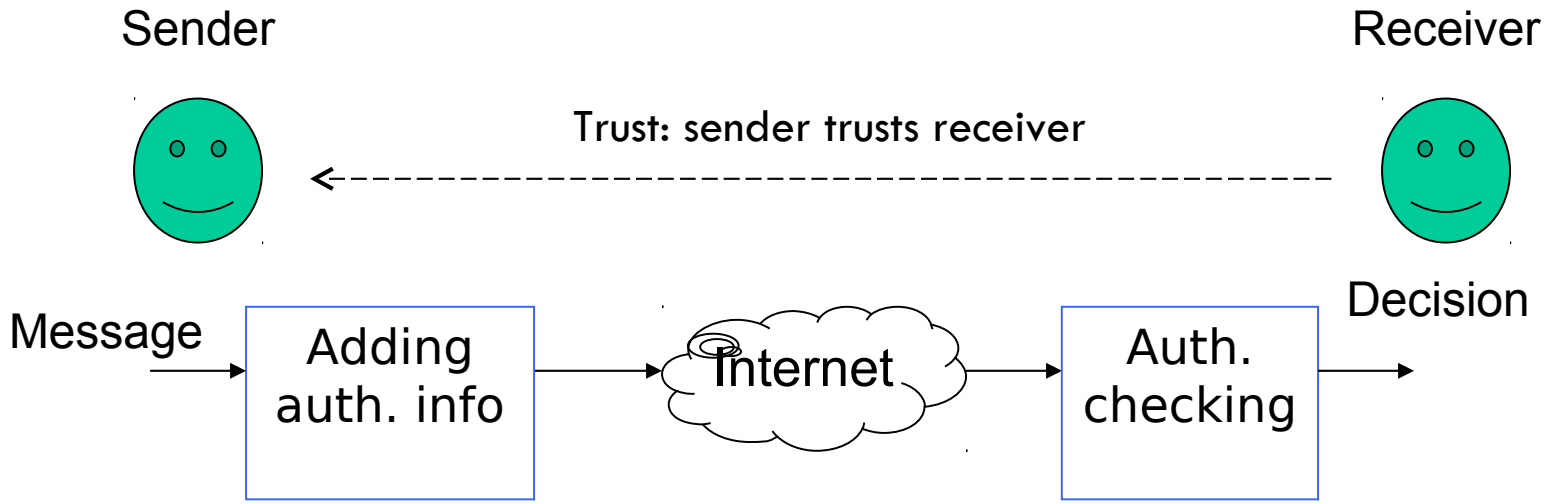
- … is the difference whether communicating parties trust each other
- No trust = need to gather evidence

- Traditional PKI enables trusting parties to authenticate over the Internet, but does not support gathering of evidence

Tidbits

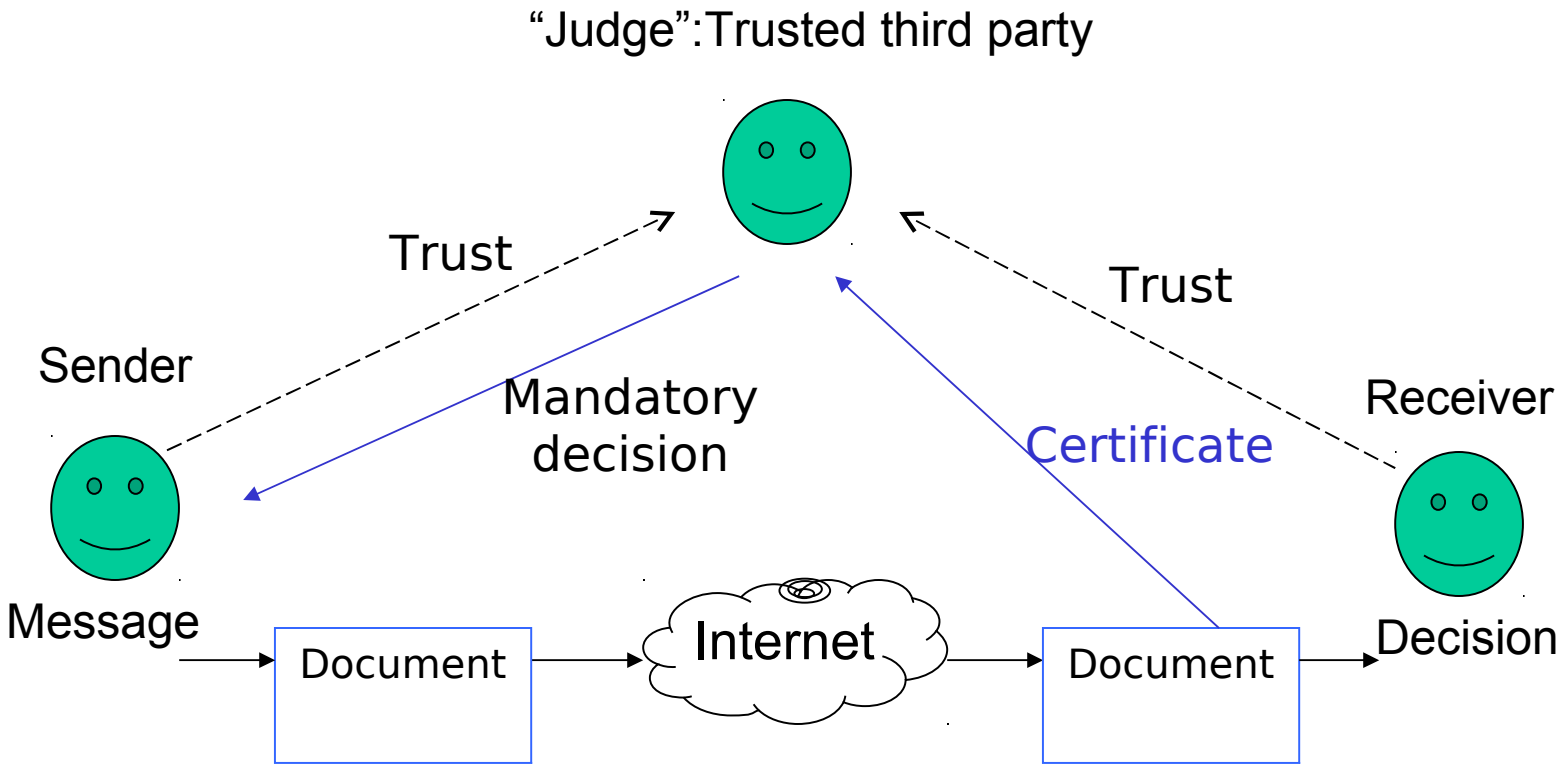
- Trusting parties do not need written contracts and gathering of evidence (signatures)
- Communication problems for trusting parties are mostly solved
- For parties without trust, gathering of evidence makes sense when there exists third party (**judge**) whose decisions are respected by both parties

Trusting Parties



- No need for evidentiary function
- Can operate without legislation support
  - Example: creating a VPN

Parties Without Trust



- Proof value is needed to reduce risks

Name-key Connection

- Must be agreed on writing to guarantee proof value of signature
- Must be available to all the potential verifiers
- Must be quickly revokable by signer
  - **Signatures created before revocation must remain valid!**
  - Example attack: sign contract, revoke certificate

Time Stamping

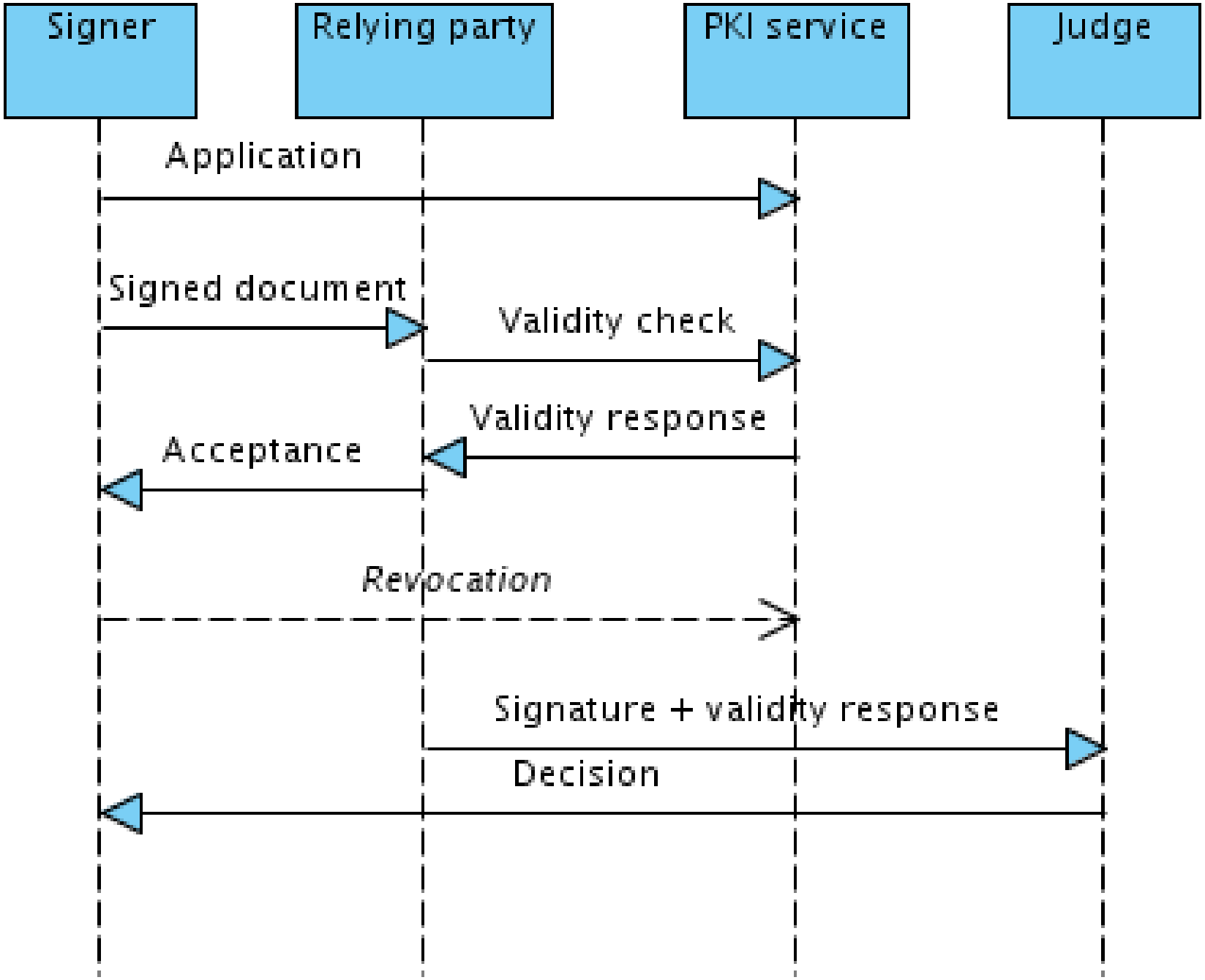
- Allows proving that data item (signature) existed at some point of time (when certificate was valid)
- Simple time stamps: (another) trusted third party signs time and hash of data
  - Must be trusted
  - Yet another signature that must be checked (and time-stamped!)

Secure Time Stamping

- Uses one-way hash functions and publication
- Proofs do not depend on third parties

Digital Document with Proof Value

- Consists of
  - Document content
  - Signature
  - Proof data
    - Certificates
    - OCSP responses
    - Time stamps
- Proof value must not depend on actions of other parties or other events not under control of the relying party

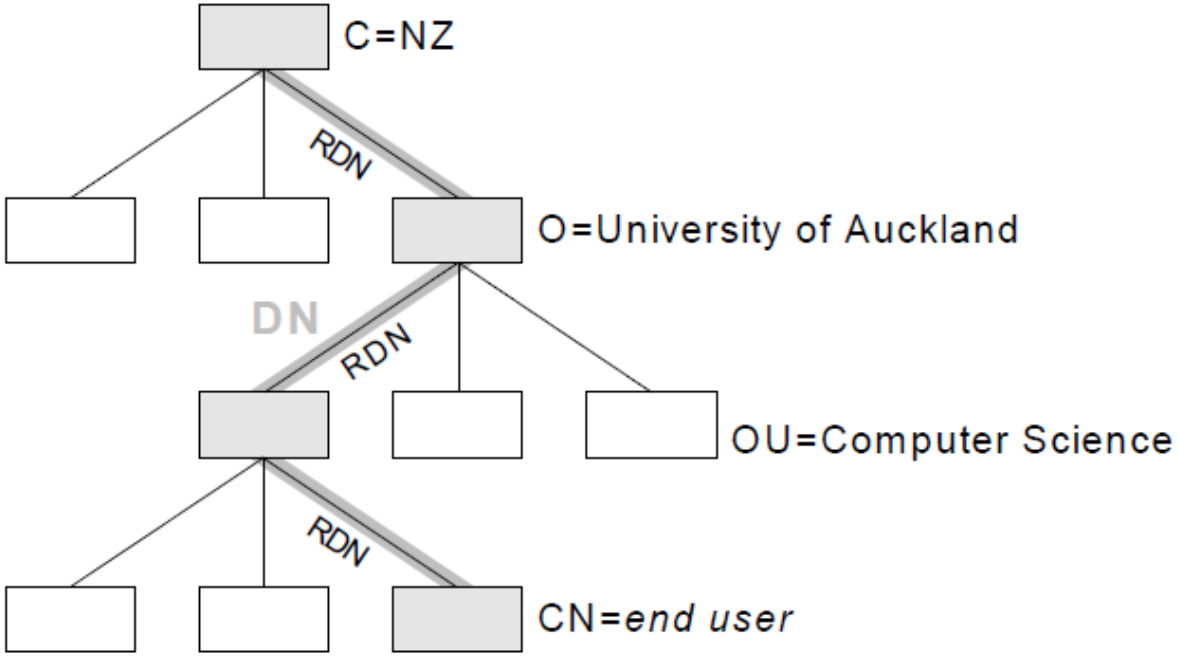

Signer
Relying party
PKI service
Judge
Application
Signed document
Validity check
Validity response
Acceptance
Revocation
Signature + validity response
Decision

Technical Info

First PKI Standards

- X.500 – directory standard
  - Created by OSI
  - Global, hierarchical telephone book
  - Maintained by monopoly telcos
  - Path through database is a series of Relative Distinguished Names
  - Collection of RDNs is Distinguished Name
- Survives today as LDAP
  - Many compatible products, e.g. Microsoft Active Directory

The Directory



- Search key: C=NZ, O=University of Auckland, OU = Computer Science, CN = foo

X.509

- **The** standard for certificates
- Public key certificate
- CRL
- Attribute certificate
  - Can be used to bind attributes to name
  - Attributes change faster than name
  - Frequency of certificate change is proportional to the square of number of attributes

X.509 (2)

- Very general and vague
- Contains just data structure descriptions
- Usually organizations create **profiles** which are more specific
  - What fields can be used
  - How to process certificates
  - What certificates mean

X.509 (3)

- Global X.500 directory was never developed
- X.509 certs were intended to be used for directory access control

- We still carry the technological baggage

PKIX

- Using X.509 certificates for the Internet
- Important restrictions and clarifications to the X.509 standard
- Additional useful protocols
  - Online Certificate Status Protocol
  - Time-Stamping Protocol
  - Server-based Certificate Validation Protocol

OCSP

- Signed response by trusted third party
  - Contains certificate number and status code
  - Status = good, revoked, unknown
- good = **not revoked**!
  - Does not directly answer the question: is this cert valid
- OCSP responses contain validity times
  - Allows precomputing or caching of responses

OCSP (2)

- Protocol design coal: backward compatibility with CRLs
- Possible build OCSP server that uses CRLs as source of information

TSP

- Very simple hash-and-sign protocol
- Client sends hash of data
- Server signs hash together with current time

- Server is fully trusted
  - Can back-date documents
- Problem: how to verify the servers' signature later?

SCVP

- One of several OCSP-like online verification protocols
- Delegated Path Discovery
  - Server finds all the necessary certificates and validation info
  - Client performs validation
- Delegated Path Validation
  - Server finds all the necessary information and performs validation
  - Server becomes trusted party

Conclusion

- Current PKI protocols are developed based on assumptions that have not been valid for decades
- Next lecture: more PKI protocols and troubles in paradise